Avis sur la demande de consultation préalable du Parquet européen concernant les risques identifiés dans l'analyse d'impact relative à la protection des données de son système de gestion des dossiers

1. PROCÉDURE

Le 24 juillet 2020, le Contrôleur européen de la protection des données (CEPD) a reçu une demande de consultation préalable au titre de l'article 72, paragraphe 1, point a), du règlement (UE) 2017/1939 du 12 octobre 2017[1] (ci-après le «règlement») concernant l'analyse d'impact relative à la protection des données (AIPD) du système de gestion des dossiers, réalisée conformément à l'article 71 du règlement.

La notification envoyée par le Parquet européen contenait une description de l'environnement de traitement, une évaluation de la nécessité et de la proportionnalité, ainsi qu'une analyse des risques et des mesures d'atténuation des risques[2]. Le Parquet européen a joint à l'AIPD les documents suivants:

[EXPURGÉ]

Le CEPD se réjouit du fait que, comme indiqué dans la conclusion de l'AIPD, le Parquet européen ait tenu compte des exigences en matière de protection des données lors de la phase de conception et de mise en œuvre du système de gestion des dossiers ([EXPURGÉ]).

Conformément à l'article 72, paragraphe 4, du règlement, le CEPD doit donner son avis dans un délai maximal de six semaines à compter de la réception de la demande de consultation, avec une possibilité de prolongation d'un mois. La notification a été reçue le 24 juillet 2020. Compte tenu de la complexité du traitement envisagé, le CEPD a informé le Parquet européen le 18 août 2020 que le délai serait prolongé d'un mois. Le CEPD rendra donc son avis au plus tard le **5 octobre 2020**.

[1] JO L 283 du 31.10.2017, p. 1–71.

[2] Conformément à l'article 71, paragraphe 2, du règlement, «[l]'analyse visée au paragraphe 1 contient au moins une **description générale des opérations de traitement envisagées**, une **évaluation des risques** pour les droits et les libertés des personnes concernées, les **mesures envisagées** pour faire face à ces risques, les **garanties**, **mesures et mécanismes de sécurité** visant à assurer la protection des données opérationnelles à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées».

2. DESCRIPTION DU TRAITEMENT

Le Parquet européen a été institué par le règlement et est compétent pour rechercher, poursuivre et renvoyer en jugement les auteurs d'infractions pénales portant atteinte au budget de l'UE, comme la fraude, la corruption ou les formes graves de fraude transfrontière à la TVA.

En tant qu'agence de l'UE qui exerce des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité FUE, le Parquet européen traite des données opérationnelles à caractère personnel conformément aux règles établies dans le règlement et dans son règlement intérieur. Les données opérationnelles à caractère personnel sont traitées au moyen d'un système de gestion des dossiers, conformément à l'article 44 du règlement.

Le système de gestion des dossiers du Parquet européen est établi en vertu de l'article 44 du règlement, qui dispose qu'il sera géré conformément aux règles fixées dans le règlement et dans le règlement intérieur du Parquet européen. Aux termes de l'article 44, paragraphe 4, du règlement, le système de gestion des dossiers comprend: un registre des informations obtenues par le Parquet européen conformément à l'article 24; un index de tous les dossiers; et toutes les informations provenant des dossiers stockés sous forme électronique. Le Parquet européen a l'intention de rendre son système de gestion des dossiers opérationnel dans les prochains mois.

3. ÉVALUATION JURIDIQUE ET TECHNIQUE

3.1. Nécessité d'une consultation préalable conformément à l'article 72 du règlement

L'article 72 du règlement subordonne le traitement qui fera partie d'un nouveau fichier à une consultation préalable du CEPD:

a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 71, indique que le traitement présenterait un risque élevé si le Parquet européen ne prenait pas de mesures pour atténuer le risque; ou
b) lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les droits et libertés des personnes concernées.

Comme indiqué dans l'AIPD[3], le traitement de données opérationnelles dans le système de gestion des dossiers poursuit une finalité judiciaire et répressive, qui est, par définition, une opération de traitement présentant un risque intrinsèque élevé pour les personnes concernées. En outre, l'AIPD met en évidence des risques élevés en l'absence d'adoption par le Parquet européen de mesures d'atténuation des risques identifiés. Cela entraîne donc l'obligation pour le Parquet européen de consulter le CEPD, conformément à l'article 72, paragraphe 1, point a), du règlement. En outre, une consultation préalable est également nécessaire au titre de l'article 71, paragraphe 1, point b), du règlement, étant donné que ce type de traitement, qui utilise de nouveaux mécanismes et procédures, comporte en soi des risques élevés pour les droits et libertés des personnes concernées en raison de la nature des données traitées et de leur incidence potentielle sur le droit à la protection des données et d'autres droits fondamentaux

[3] Page 5.

des personnes concernées, tels que la non-discrimination, le droit à un recours effectif et à un procès équitable, la présomption d'innocence et les droits de la défense.

3.2. Portée de l'avis

L'avis du CEPD sur cette consultation préalable **ne concerne que l'AIPD telle qu'elle est décrite dans la notification** du 24 juillet 2020 (V4.0) et la documentation jointe.

Le présent avis se concentrera sur les aspects essentiels qui soulèvent des problèmes de conformité avec le cadre juridique applicable en matière de protection des données ou qui méritent une analyse plus approfondie.

À ce stade, le CEPD ne formulera pas d'observations spécifiques sur la documentation présentée avec l'AIPD. Le CEPD a déjà formulé des observations et des recommandations sur le règlement intérieur du Parquet européen [dossier CEPD: 2020-0781] et sur les règles du Parquet européen relatives au traitement de données à caractère personnel [dossier CEPD: 2020-0782][4]. Le CEPD se réjouit de toute demande ultérieure de consultation émanant du Parquet européen.

Le CEPD relève que l'AIPD ne contient aucune disposition concernant l'accès d'Eurojust et de l'OLAF aux informations figurant dans le système de gestion des dossiers du Parquet européen sur la base d'un système de concordance/non-concordance (*hit/no-hit*) (comme le prévoient, respectivement, l'article 100, paragraphe 3, et l'article 101, paragraphe 5, du règlement). Si le Parquet européen devait mettre en œuvre une telle fonction dans son système de gestion des dossiers, le CEPD s'attend à être consulté, conformément à l'article 72 du règlement.

Le CEPD s'attend également à être consulté à l'égard de toute mise à jour importante de l'AIPD à la suite d'une modification substantielle des opérations de traitement de données à caractère personnel dans le système de gestion des dossiers.

3.3. Base juridique du traitement

La finalité du traitement relève de l'**article 44** du règlement qui dispose que le Parquet européen établit un système de gestion des dossiers ayant pour objectifs de:

a) fournir un soutien à la conduite des enquêtes et des poursuites menées par le Parquet européen;
b) garantir un accès sécurisé aux informations relatives aux enquêtes et aux poursuites au sein du Bureau central et par les procureurs européens délégués;
c) permettre le recoupement d'informations et l'extraction de données à des fins d'analyse opérationnelle et de statistiques;

[4] Voir la lettre du CEPD au chef du Parquet européen du 17 septembre 2020 et les observations jointes.

d) faciliter le contrôle en vue de s'assurer que le traitement des données opérationnelles à caractère personnel est licite et conforme aux dispositions pertinentes du règlement.

3.4. Évaluation de l'AIPD

Le Parquet européen a identifié un certain nombre de risques pour les personnes concernées. Les mesures d'atténuation des risques identifiés comprennent, selon l'AIPD, des mesures techniques (spécifications de conception et structure du système de gestion des dossiers), organisationnelles ou juridiques (règles de mise en œuvre ayant une valeur juridique au sein du Parquet européen, telles que le règlement intérieur, les règles internes relatives au traitement des données à caractère personnel ou les règles relatives à la protection des informations sensibles non classifiées).

Le Parquet européen a conclu que «les mesures en place, qu'elles soient organisationnelles, techniques ou juridiques, réduisent les risques résiduels et globaux à un niveau acceptable et proportionné par rapport à la finalité des traitements et pour le Parquet européen [...]»[5].

Tout d'abord, le CEPD tient à souligner l'excellente qualité de l'AIPD en ce qui concerne la méthodologie utilisée (y compris les facteurs de risque et la matrice sur la probabilité et l'impact) ainsi que sur le fond (description de la situation et analyse, les personnes concernées étant notamment placées au centre de chaque risque). Le CEPD apprécie tout particulièrement le fait que le Parquet européen ait centré son analyse sur les risques pour les personnes concernées.

Le CEPD examinera ci-après les **principales questions relatives à la protection des données** résultant du traitement de données à caractère personnel en cause, eu égard aux mesures envisagées par le Parquet européen pour faire face aux risques en matière de protection des données. Par ailleurs, l'impact sur **d'autres droits fondamentaux** des personnes concernées est également pris en considération. Le CEPD prend note du fait que, lors de l'identification et de la description des risques, le Parquet européen a tenu compte (bien que sans les nommer spécifiquement) de risques pour d'autres droits fondamentaux que la protection des données.

Tout en reconnaissant la qualité globale de l'AIPD, le CEPD formule un certain nombre d'observations et de recommandations spécifiques sur la méthodologie (section 3.4.1) et sur les risques identifiés par le Parquet européen (section 3.4.2).

3.4.1. Méthodologie de l'AIPD

a) **Regroupement des «événements» et des «risques»**

L'AIPD comporte une colonne intitulée «**Événement/Risque**». Toutefois, les «événements» et les «risques» sont deux notions différentes: alors qu'un «événement» a un impact et une probabilité, un «risque» découle d'un événement et constitue un résultat possible (généralement négatif) d'un événement. La terminologie du document devrait donc être

[5] Page 5.

adaptée de manière à ce que les événements ne soient pas mélangés aux risques (le tableau 7.2, deuxième colonne, de l'AIPD devrait faire référence exclusivement aux «événements»). Par ailleurs, le contenu du tableau 7.2, quatrième colonne («Risque pour la personne concernée») de l'AIPD devrait décrire les risques associés à chaque événement et se concentrer uniquement sur ceux-ci.

Recommandation nº 1: adapter l'AIPD afin de tenir compte de la différence conceptuelle entre les «événements» et les «risques».

b) **De manière générale, les mesures d'atténuation ne sont pas suffisamment détaillées**

Dans la plupart des cas, les mesures d'atténuation figurant dans l'AIPD restent d'une teneur relativement générale et ne précisent donc pas concrètement comment le risque identifié sera traité et quelle mesure d'atténuation concrète sera spécifiquement appliquée. Cela s'explique en partie par l'association susmentionnée entre les «événements» et les «risques» et par le fait que, parfois, l'analyse ne décrit pas comment un risque peut se matérialiser, ce qui implique que la mesure d'atténuation ne peut pas être suffisamment précise. En particulier, bien que des règles spécifiques figurant dans les règles internes du Parquet européen (comme le règlement intérieur ou les règles internes relatives au traitement de données à caractère personnel ou les règles relatives au délégué à la protection des données) puissent concerner les risques identifiés, il est souvent difficile de déterminer quelle disposition spécifique des règles susvisées s'appliquera dans un cas particulier et comment le risque sera atténué concrètement.

À titre d'exemple, le **risque nº 34** mentionné dans l'AIPD fait référence au fait que «**les violations de données à caractère personnel ne sont pas dûment notifiées et suivies d'une réaction**». Les mesures d'atténuation de ce risque mentionnent les «règles relatives au traitement de données à caractère personnel, le règlement intérieur, la participation du DPD à la procédure et sa consultation».

Recommandation nº 2: inclure dans la section relative à l'atténuation de chaque risque identifié, lorsque cela n'a pas encore été fait, la description des mesures spécifiques destinées à traiter le risque particulier (telles que des mesures techniques et organisationnelles et, chaque fois que cela est mis en œuvre dans le système de gestion des dossiers, la mesure d'atténuation devrait décrire la fonctionnalité) et la référence spécifique aux règles internes applicables.

Recommandation nº 3: afin de dûment notifier et, le cas échéant, de communiquer les violations de données à caractère personnel et d'agir pour atténuer les risques pour les personnes concernées, concevoir et élaborer une **politique relative aux violations de données à caractère personnel** présentant les éléments essentiels, tels que les rôles et les fonctions qui doivent intervenir en cas d'incident de sécurité ou de violation de données à caractère personnel, l'évaluation des risques, des procédures de notification au CEPD et, le cas échéant, la communication aux personnes concernées, ainsi que des mesures appropriées d'atténuation des risques.

c) **Intitulé de la colonne – «Principe sous-jacent en matière de protection des données» – ne reflétant pas son contenu**

Le contenu de la colonne «Principe sous-jacent en matière de protection des données» du tableau 7.2 ne fait pas uniquement référence aux principes relatifs à la protection des données, qui sont, *stricto sensu*, les principes énumérés à l'article 47 du règlement. Cette colonne comprend également, par exemple, des références à l'exercice des droits des personnes concernées, à la communication d'une violation de données, aux transferts, c'est-à-dire à des règles générales en matière de protection des données.

Recommandation nº 4: adapter l'intitulé de la colonne susvisée afin d'indiquer qu'elle fait référence aux règles générales en matière de protection des données.

d) **Des aspects essentiels concernant le réexamen de l'AIPD font défaut**

[EXPURGÉ]

Bien qu'elle fasse référence à la nécessité de réexaminer l'AIPD dans certaines circonstances, l'AIPD ne contient pas d'informations sur la fréquence de son réexamen périodique, sur les critères qui déclenchent un réexamen non périodique ainsi que sur les entités chargées du réexamen.

Recommandation nº 5: inclure une **référence à la fréquence du réexamen de l'AIPD** après la mise en service du système de gestion des dossiers. Compte tenu des considérations qui précèdent, le CEPD recommande que l'AIPD soit réexaminée chaque année, ainsi que chaque fois que se produit une évolution majeure qui l'affecte. L'AIPD doit également préciser **la ou les entités chargées** d'engager la procédure de réexamen et de procéder à la mise à jour (à savoir le responsable du traitement, le porteur du projet), ainsi que les **critères du réexamen non périodique** (à savoir lorsque des modifications importantes du système de gestion des dossiers sont proposées; en cas d'incidents de sécurité graves ou de changements dans l'environnement de sécurité).

3.4.2. Risques

a) Certains risques identifiés dans l'AIPD doivent être clarifiés

Le Parquet européen devrait donner davantage de précisions concernant certains des risques identifiés dans l'AIPD.

- Le **risque nº 10** concerne le fait de ne pas **informer correctement les personnes concernées** du traitement de données les concernant. Les mesures d'atténuation prévues dans l'AIPD consistent à indiquer dans le système de gestion des dossiers si les informations ont été fournies ou, dans la négative, pourquoi une limitation a été appliquée. Toutefois, les mesures d'atténuation mentionnées ne tiennent pas compte des cas où «la suspension ou le retard dans l'information de la personne concernée» (comme le prévoit l'article 4, paragraphe 5, des règles

internes du Parquet européen relatives à la protection des données) n'est plus valable et où la personne concernée n'aurait toujours pas été informée.

Recommandation nº 6: analyser et donner davantage de précisions concernant les cas dans lesquels le **report de l'information** des personnes concernées n'est plus valable et, partant, concevoir et mettre en œuvre des mesures d'atténuation appropriées pour que la personne concernée soit dûment informée dans ces cas.

- Le **risque nº 12** fait référence à l'information des personnes concernées quant à une «**atteinte à la sécurité**».

  L'article 75, paragraphe 1, du règlement dispose ce qui suit: «Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le Parquet européen communique la violation à la personne concernée sans retard indu». L'article 8 des règles internes du Parquet européen relatives à la protection des données précise en outre les conditions de communication aux personnes concernées d'une violation de leurs données à caractère personnel. Dans un souci de clarté, le Parquet européen devrait harmoniser la terminologie, à savoir que la description de l'événement devrait faire référence à une «violation de données à caractère personnel» plutôt qu'à une «atteinte à la sécurité».

Recommandation nº 7: préciser que:

- l'événement fait référence à une «violation de données à caractère personnel»;

- le risque fait référence à l'information des personnes concernées quant à une **violation de leurs données à caractère personnel**, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques concernées.

- Le **risque nº 22** («**Les données à caractère personnel sont introduites dans le système de gestion des dossiers sans contexte/distinction entre, par exemple, le rôle des personnes concernées**») contient la description suivante du risque pour la personne concernée: «Les **personnes concernées** qui sont mentionnées dans la liste, par exemple comme des suspects plutôt que comme des témoins, ou des témoins qui ne sont pas identifiés en tant que tels, mais font l'objet d'un traitement plus invasif».

  Si la définition du risque fait référence à des situations dans lesquelles des données à caractère personnel sont introduites sans opérer de distinction entre les rôles des personnes concernées, la description du risque fait référence à la possibilité d'identifier erronément des personnes concernées. Par ailleurs, la mesure d'atténuation n'aborde pas le problème mentionné dans la définition du risque, mais uniquement les cas où des données ou des métadonnées font défaut, alors qu'un risque important concerne des situations où l'identification des personnes concernées est incorrecte.

Recommandation nº 8: préciser le ou les risques relatifs à l'introduction de données à caractère personnel dans le système de gestion des dossiers. De l'avis du CEPD, l'absence de métadonnées et une identification erronée des personnes concernées sont possibles et devraient être traitées de manière adéquate comme des risques distincts pour les personnes concernées, et des mesures d'atténuation appropriées devraient être prévues pour chacun de ces risques.

- Le **risque nº 24** («**Des données à caractère personnel dont l'inexactitude, le caractère incomplet ou le traitement illicite sont connus sont transférées/fournies à des tiers**») contient la description suivante du risque pour la personne concernée: «Lorsque les données d'une personne concernée ont été traitées de manière irrégulière, il n'appartient pas à la personne concernée de s'adresser à d'autres destinataires, mais cela relève de la responsabilité du Parquet européen».

  La description du risque ne correspond pas à l'événement mentionné. À titre d'exemple, si les données transférées devaient être inexactes, un risque pour les personnes concernées est qu'elles pourraient faire l'objet d'enquêtes et/ou de jugements erronés par le destinataire des données.

Recommandation nº 9: clarifier la description du risque de sorte que le risque pour les personnes concernées soit correctement identifié, décrit et traité.

- Le **risque nº 25** fait référence au fait que le CEPD «**est dans l'incapacité d'accéder aux données à caractère personnel ou aux journaux de traitement qu'il a demandés**». La description du risque est la suivante: «La capacité de contrôle du CEPD est compromise si l'accès auquel il a droit ne peut être fourni» et le «Principe sous-jacent en matière de protection des données» est un « Contrôle du CEPD».

  Si le risque identifié dans l'AIPD met l'accent sur le contrôle du CEPD, le risque pour la personne concernée n'est pas correctement décrit. À titre d'exemple, l'un des risques pour les personnes concernées est le fait qu'elles pourraient ne pas être en mesure d'exercer leurs droits par l'intermédiaire du CEPD, comme le prévoit l'article 62 du règlement.

Recommandation nº 10: adapter la description du risque, pour tenir compte du risque pour les personnes concernées, ainsi que le contenu de la colonne «Principe sous-jacent en matière de protection des données».

- Le **risque nº 28** fait référence au fait que «**le DPD du Parquet européen [n'est] pas en mesure d'accéder aux données à caractère personnel nécessaires à l'exercice de sa fonction**». La description du risque est la suivante: «La capacité de contrôle du DPD est compromise si l'accès auquel il a droit ne peut être fourni» et le «Principe sous-jacent en matière de protection des données» est un «Contrôle».

  Si le risque identifié dans l'AIPD met l'accent sur le contrôle du DPD, le risque pour la personne concernée n'est pas correctement décrit. À titre d'exemple, l'un des risques pour les personnes concernées est le fait qu'elles pourraient ne pas être en mesure de bénéficier du contrôle indépendant du respect du cadre juridique relatif à la protection des données que réalise le DPD, tel que décrit en détail à l'article 79 du règlement.

Recommandation nº 11: adapter la description du risque, pour tenir compte du risque pour les personnes concernées, ainsi que le contenu de la colonne «Principe sous-jacent en matière de protection des données».

- Le **risque nº 29** fait référence au fait que la «**possibilité d'accorder un accès personnel ciblé n'est pas prévue, de sorte que chacun peut avoir accès**». La description du risque est la

suivante: «La divulgation inutile de données à caractère personnel augmente le risque résiduel par rapport à la non-divulgation».

Recommandation nº 12: clarifier la définition et la description du risque identifié, par exemple par une référence au fait que les niveaux d'accès ne sont pas définis précisément sur la base du besoin d'en connaître. Clarifier également la description du risque en se concentrant sur le risque pour les personnes concernées.

- Le **risque 32** fait référence au fait que «**des catégories particulières de données à caractère personnel sont traitées sans justification**». La description du risque est la suivante: «Des limitations spécifiques s'appliquent au traitement de catégories particulières de données à caractère personnel. Lorsque ces catégories ne sont pas identifiées en tant que telles, elles peuvent bénéficier d'une protection moindre».

  La définition et la description du risque ne permettent pas de déterminer si le risque concerne le traitement illicite de catégories particulières de données à caractère personnel (comme indiqué dans la définition) ou le fait que des catégories particulières de données à caractère personnel «ne sont pas identifiées en tant que telles» (comme indiqué dans la description).

Recommandation nº 13: clarifier la définition et la description du risque susvisé, en identifiant et en soulignant précisément les risques pour les personnes concernées, qui peuvent inclure (sans toutefois s'y limiter) le fait que, lorsque les données ne sont pas correctement identifiées comme relevant de catégories particulières de données à caractère personnel, les personnes concernées pourraient bénéficier d'une protection moindre.

b) Certains risques ont été négligés dans l'AIPD

Le CEPD recommande que le Parquet européen prenne en considération un certain nombre de risques supplémentaires. Le CEPD a identifié ces risques supplémentaires en se fondant sur la description du processus dans l'AIPD, sur les risques mentionnés dans cette analyse et sur la documentation de référence présentée. Néanmoins, le CEPD ne considère pas que l'ajout de ces risques à l'AIPD rendrait l'analyse des risques nécessairement exhaustive. Le Parquet européen est invité à examiner, à ce stade et par la suite, si ce traitement de données à caractère personnel entraîne d'autres risques pour les personnes concernées, lesquels devraient être inclus et abordés dans un futur réexamen de l'AIPD.

- **Risque supplémentaire nº 1: non-respect de l'obligation de ne traiter que des données relevant du domaine de compétence du Parquet européen (licéité)**

  L'article 24, paragraphe 7, du règlement dispose que «[s]i, après vérification, le Parquet européen décide qu'il n'y a pas lieu d'ouvrir une enquête [...] ou d'exercer son droit d'évocation [...], les motifs de sa décision sont enregistrés dans le système de gestion des dossiers». De même, le second alinéa de la même disposition prévoit que «[l]e Parquet européen informe l'autorité qui a signalé le comportement délictueux conformément au paragraphe 1 ou 2, ainsi que les victimes de l'infraction et, si le droit national en dispose ainsi, les autres personnes qui ont signalé le comportement délictueux». Par ailleurs, l'article 24, paragraphe 8, du règlement dispose que, «[s]'il vient à la connaissance du Parquet européen qu'une infraction pénale ne

relevant pas de sa compétence pourrait avoir été commise, celui-ci en informe les autorités nationales compétentes sans retard indu et leur transmet tous les éléments de preuve pertinents».

Conformément à l'article 49, paragraphe 4, du règlement, «[l]e Parquet européen peut traiter temporairement des données opérationnelles à caractère personnel afin de déterminer si ces données sont pertinentes pour ses tâches et pour [s]es finalités. Le collège, [...] après consultation du Contrôleur européen de la protection des données, précise davantage les conditions applicables au traitement de ces données à caractère personnel, en particulier en ce qui concerne l'accès à ces données opérationnelles et leur utilisation, ainsi que les délais afférents à leur conservation et à leur effacement».

L'article 37, paragraphe 6, du projet de règlement intérieur du Parquet européen précise que «[EXPURGÉ]».

À la section *5.7.1. Saisie et enregistrement des données opérationnelles à caractère personnel*, *Figure 18 – Tableau récapitulatif pour la vérification et l'enregistrement* de l'AIPD, il est indiqué que: «Les informations conservées sont évaluées par le personnel compétent du Parquet européen si elles relèvent de son mandat. Dans le cas contraire, les informations sont rejetées et le fournisseur en est éventuellement informé et/ou les données sont transmises à l'autorité compétente, à l'organe de l'UE ou une autre mesure est prise».

S'agissant du processus de vérification du rapport entre les données à caractère personnel reçues et les tâches et objectifs du Parquet européen, l'AIPD relève le risque suivant: risque nº 1: «Les données à caractère personnel sont traitées de manière illicite en l'absence de toute base juridique pour le traitement», avec le risque qui en découle pour la personne concernée: «Les données à caractère personnel faisant l'objet d'un traitement illicite n'offrent pas de protection ou de garantie à la personne concernée et la privent de ses droits à la protection des données à caractère personnel». Les mesures d'atténuation comprennent: «un processus détaillé pour l'introduction des données à caractère personnel dans le système de gestion des dossiers, conformément au titre III du règlement intérieur (articles 37 et suivants)».

Sur la base de la description figurant dans l'AIPD et plus particulièrement à la *figure 18*, ainsi que des dispositions mentionnées à l'article 37, paragraphe 6, du projet de règlement intérieur du Parquet européen et afin de tenir dûment compte des risques pour les personnes concernées et d'éviter les risques qui pourraient résulter d'une ambiguïté dans la procédure, il convient d'apporter des précisions supplémentaires concernant les données à caractère personnel reçues par le Parquet européen mais ne relevant pas de sa compétence.

Recommandation nº 14: inclure parmi les risques la possibilité que des procédures peu claires sur la manière de traiter les données à caractère personnel reçues et traitées temporairement par le Parquet européen mais ne relevant pas de son mandat puissent engendrer des risques pour les personnes concernées (par exemple, il n'existe pas de flux de travail précis pour ces données et, plus précisément, il n'existe pas de procédure claire pour le renvoi des données au fournisseur, le transfert des données pertinentes aux autorités compétentes et les conditions spécifiques relatives à ces transferts, ainsi que pour l'effacement des données).

- **Risque supplémentaire nº 2: non-respect de l'obligation de répondre avec précision aux demandes des personnes concernées**

  L'article 59 du règlement dispose que la personne concernée a le droit d'obtenir du Parquet européen «la confirmation que des données opérationnelles à caractère personnel la concernant

sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données opérationnelles à caractère personnel» ainsi que certaines informations spécifiques.

À la section *5.7.1. Saisie et enregistrement des données opérationnelles à caractère personnel*, *Figure 18 — Tableau récapitulatif pour la vérification et l'enregistrement* de l'AIPD, il est indiqué que «[EXPURGÉ]». De même, à la section *6 Nécessité et proportionnalité*, il est indiqué que «[...] les données qui sont conservées dans le système de gestion des dossiers, mais ne sont pas encore enregistrées/vérifiées, ne sont pas accessibles à un utilisateur effectuant une recherche».

Nous prenons note du fait que cette étape procédurale vise à garantir que le Parquet européen ne traite que des données pertinentes aux fins de l'exécution de ses tâches, conformément aux dispositions de l'article 49, paragraphe 4, du règlement. Nous prenons également note du Titre III – Questions opérationnelles/Chapitre 1 – Enregistrement et vérification des informations, du projet de règlement intérieur, qui précise les dispositions applicables à ce traitement temporaire de données à caractère personnel[6].

En tout état de cause, bien qu'il soit temporaire, il s'agit d'un traitement de données à caractère personnel et, de ce fait, les dispositions relatives à la protection des données lui sont pleinement applicables. À titre d'exemple, si une personne concernée cherche à savoir si des données opérationnelles à caractère personnel la concernant sont traitées et demande l'accès à ses données à caractère personnel, le Parquet européen devrait être en mesure de déterminer précisément s'il traite des données à caractère personnel du demandeur.

Recommandation nº 15: inclure parmi les risques la possibilité d'un non-respect de l'obligation de répondre avec précision aux demandes des personnes concernées. Le CEPD **recommande** au Parquet européen de faire la distinction entre les données à caractère personnel enregistrées (en attente de vérification) et les données à caractère personnel non enregistrées, et d'examiner les risques liés à chacune de ces situations. Par ailleurs, le Parquet européen devrait envisager de distinguer l'enregistrement et la vérification, étant donné que ces deux étapes pourraient engendrer des risques différents.

- **Risque supplémentaire nº 3: non-respect du principe de limitation de la durée de conservation**

Conformément au principe de «limitation de la durée de conservation» [article 47, paragraphe 1, point e)], «les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées».

L'AIPD et la documentation jointe ne permettent pas de déterminer combien de temps les données à caractère personnel «[...] qui sont conservées dans le système de gestion des dossiers, mais qui ne sont pas encore enregistrées/vérifiées», seront conservées avant d'être évaluées par le personnel compétent du Parquet européen, si elles relèvent de son mandat, et avant qu'une décision ne soit prise à cet égard. L'article 49, paragraphe 4, du règlement précise effectivement que «[l]e Parquet européen peut traiter temporairement des données opérationnelles à caractère personnel afin de déterminer si ces données sont pertinentes pour ses tâches et pour les finalités [...]». En outre, il prévoit également que, à l'issue d'une

[6] Voir la lettre du CEPD au chef du Parquet européen du 17 septembre 2020 et les observations jointes [2020-0781 et 2020-0782].

procédure particulière incluant la consultation du CEPD, le collège du Parquet européen «précise davantage les conditions applicables au traitement de ces données à caractère personnel, en particulier en ce qui concerne l'accès à ces données opérationnelles et leur utilisation, ainsi que **les délais afférents à leur conservation et à leur effacement**»[7].

Recommandation nº 16: inclure parmi les risques la possibilité que les données conservées temporairement dans le système de gestion des dossiers pour être enregistrées/vérifiées, afin de déterminer si elles relèvent ou non de la compétence du Parquet européen, soient conservées en violation du principe de limitation de la durée de conservation. À titre de mesure d'atténuation, le CEPD recommande de définir des délais de conservation spécifiques applicables aux données avant qu'elles ne soient enregistrées, ainsi qu'à celles qui ont été enregistrées mais pas encore vérifiées.

- **Risque supplémentaire nº 4: des données inexactes peuvent entraîner des décisions erronées pour la personne concernée faisant l'objet d'une enquête**

  S'agissant du **risque nº 3** («**Des données inexactes peuvent être traitées**»), l'AIPD décrit le risque pour la personne concernée comme suit: «Si les données à caractère personnel sont inexactes, elles peuvent avoir pour conséquence qu'une autre personne concernée fasse l'objet de l'attention des services répressifs et d'une enquête potentielle».

Recommandation nº 17: traiter l'autre risque qui pourrait résulter du traitement de données inexactes, à savoir le fait que des décisions erronées pourraient être prises au sujet de la personne concernée faisant l'objet d'une enquête.

- **Risque supplémentaire nº 5: transferts illicites**

  Le risque que le Parquet européen **transfère** des données opérationnelles à caractère personnel vers un pays tiers ou à une organisation internationale de manière illicite, c'est-à-dire en l'absence de décision d'adéquation, de garanties appropriées ou de dérogations dans une situation donnée, n'est ni inclus ni traité dans l'AIPD.

Recommandation nº 18: inclure et traiter le risque de transfert illicite de données opérationnelles à caractère personnel vers un pays tiers ou à une organisation internationale.

- **Risque supplémentaire nº 6: responsabilité (conjointe) du traitement**

  L'AIPD ne couvre pas les risques découlant du manque de clarté dans la compréhension et la définition des rôles en matière de responsabilité du traitement et/ou de responsabilité conjointe du traitement entre le Parquet européen et les États membres participants. En effet, la possibilité d'un chevauchement des législations (au niveau de l'Union et au niveau national) est mentionnée dans l'AIPD, «étant donné que le droit national continue de s'appliquer et de régir les enquêtes et les poursuites».

[7] Caractères gras ajoutés par nous.

Recommandation nº 19: inclure les risques découlant du manque de clarté dans la compréhension et la définition des rôles en matière de **responsabilité du traitement et/ou de responsabilité conjointe du traitement** entre le Parquet européen et les États membres participants.

- **Risque supplémentaire nº 7: recours à des sous-traitants/sous-traitants ultérieurs**

L'AIPD ne couvre pas les risques découlant du recours du Parquet européen à des sous-traitants et, le cas échéant, à des sous-traitants ultérieurs. Le recours à des sous-traitants et à des sous-traitants ultérieurs augmente le risque lié au traitement de données à caractère personnel et, de ce fait, il devrait être pris en compte dans l'AIPD.

Recommandation nº 20: inclure les risques liés au recours du Parquet européen à des sous-traitants et, le cas échéant, à des sous-traitants ultérieurs.

- **Risque supplémentaire nº 8: droits d'accès**

Le **risque nº 29** identifié dans l'AIPD fait référence au fait que la «**possibilité d'accorder un accès personnel ciblé n'est pas prévue, de sorte que chacun peut avoir accès**». Un certain nombre de risques supplémentaires liés aux droits d'accès au système de gestion des dossiers devraient être pris en compte, tels que: un accès a été accordé par erreur à des personnes qui ne devraient pas posséder ce type d'accréditation; l'accès n'est pas supprimé lorsqu'une personne n'est plus impliquée dans un dossier donné; aucun contrôle périodique d'attribution des rôles n'est effectué.

Recommandation nº 21: examiner dans l'AIPD les risques susvisés relatifs aux droits d'accès au système de gestion des dossiers.

c) Dans certains cas, l'impact des risques semble sous-évalué

Le CEPD recommande que le Parquet européen réévalue l'impact des risques suivants mentionnés dans l'AIPD.

- **Impact des risques à réévaluer nº 1:**

S'agissant du **risque nº 3** («**Des données inexactes peuvent être traitées**»), l'AIPD décrit le risque pour la personne concernée comme suit: «Si les données à caractère personnel sont inexactes, elles peuvent avoir pour conséquence qu'une autre personne concernée fasse l'objet de l'attention des services répressifs et d'une enquête potentielle». L'impact identifié dans l'AIPD est de 3.

Recommandation nº 22: réévaluer l'impact de ce risque (et le risque supplémentaire proposé par le CEPD concernant le traitement de données inexactes) et déterminer si l'impact de la prise de décisions fondées sur des données inexactes ne pourrait pas être plus important pour les personnes concernées. Si le Parquet européen devait estimer que l'impact est effectivement de 3, le CEPD attend une justification de ce niveau.

- **Impact des risques à réévaluer nº 2:**

  S'agissant du **risque nº 4** (**«Des données à caractère personnel peuvent continuer d'être traitées après l'expiration des délais prévus ou lorsqu'elles ne sont plus nécessaires»**), l'AIPD décrit le risque pour la personne concernée comme suit: «[...] Étant donné que l'absence de nécessité indique, en tout état de cause, l'absence de focalisation sur les données, la poursuite de ce traitement n'apporte aucune donnée supplémentaire concrète». L'impact identifié dans l'AIPD est de 1.

  Le CEPD estime qu'en n'appliquant pas le délai de conservation approprié, l'impact sur les personnes concernées pourrait être supérieur. En outre, il est essentiel de définir et d'appliquer des délais et des mécanismes appropriés de conservation dans le système de gestion des dossiers afin de signaler et d'effacer les données lorsqu'elles ne sont plus nécessaires.

Recommandation nº 23: réévaluer l'impact du risque lié à une durée de conservation excessive et déterminer si son impact pour les personnes concernées ne pourrait pas être supérieur. Si le Parquet européen devait estimer que l'impact est effectivement de 1, le CEPD attend une justification de ce niveau.

d) La probabilité résiduelle de réalisation du risque après atténuation est sous-estimée (risque nº 14 – Incertitude concernant le cadre juridique applicable)

Il ressort de l'AIPD qu'après application des mesures d'atténuation, la probabilité résiduelle du **risque nº 14 («Incertitude concernant le cadre juridique applicable au traitement de leurs données à caractère personnel»)** est de 1 (la probabilité initiale, avant atténuation, est de 4). Compte tenu de la complexité du cadre juridique applicable (cadre juridique de l'Union et droit national applicable – législations mettant en œuvre la directive relative à la protection des données dans le domaine répressif en plus du droit procédural national applicable et possibilité d'avoir plusieurs droits nationaux applicables, comme le droit de la procédure pénale), le CEPD se demande si le risque résiduel n'est pas sous-estimé.

Recommandation nº 24: réévaluer si la probabilité résiduelle de réalisation du risque peut effectivement être réduite à 1 après l'application des mesures d'atténuation, en cas d'incertitude quant au cadre juridique applicable.

e) Les mesures d'atténuation du risque ne réduisent pas la probabilité résiduelle de réalisation du risque (risque nº 25 – incapacité du CEPD d'accéder aux données à caractère personnel/journaux)

Il ressort de l'AIPD qu'après application des mesures d'atténuation, la probabilité résiduelle de réalisation du **risque nº 25** (le CEPD **«n'est pas en mesure d'accéder aux données à caractère personnel ou aux journaux des traitements qu'il a demandés»**) conserve la même valeur, à savoir 2.

Recommandation nº 25: réévaluer les mesures d'atténuation afin de réduire la probabilité résiduelle de réalisation du risque après l'application des mesures d'atténuation.

3.5. Évaluation des risques relatifs à la sécurité de l'information

[EXPURGÉ]

Recommandation nº 26: [EXPURGÉ]

***

4. RECOMMANDATIONS

Le CEPD tient tout d'abord à souligner la qualité globale de l'AIPD. Tout en reconnaissant cet aspect positif, le CEPD a formulé plusieurs recommandations visant à garantir la conformité avec le règlement. Le CEPD s'attend à ce que les **recommandations susvisées (résumées ci-dessous) soient mises en œuvre et que les preuves documentaires** de cette mise en œuvre soient fournies dans un délai de **trois mois** à compter de la date du présent avis.

1. Faire en sorte que l'AIPD soit adaptée afin de tenir compte de la différence conceptuelle entre les «**événements**» et les «**risques**» (recommandation nº 1).
2. Faire en sorte que la section relative à l'**atténuation** de chaque risque identifié inclue la description des mesures spécifiques destinées à traiter le risque particulier identifié (recommandations nº 2 et 3).
3. Adapter l'intitulé de la colonne «**Principe sous-jacent en matière de protection des données**» afin de faire référence aux règles générales de protection des données (recommandation nº 4).
4. Faire en sorte que l'AIPD inclue une référence à la fréquence du **réexamen** de l'AIPD après la mise en service du système de gestion des dossiers, aux **entités** chargées d'engager le processus de réexamen et de procéder à la mise à jour, ainsi qu'aux **critères applicables au réexamen non périodique** (recommandation nº 5).
5. Préciser les **risques** mentionnés à la section e) de l'avis (recommandations nº 6 à 13).
6. Examiner les **risques supplémentaires** mentionnés à la section f) de l'avis (recommandations nº 14 à 22).
7. Réévaluer l'**impact** de certains risques mentionnés à la section g) de l'avis (recommandations nº 23 et 24). En ce qui concerne ces recommandations, le CEPD s'attend à recevoir une justification de l'impact actuel identifié dans l'AIPD ou des preuves documentaires de mise en œuvre.

8. Réévaluer si, dans le cas du risque nº 14, la **probabilité résiduelle** de réalisation du risque peut effectivement être réduite à 1 après l'application des mesures d'atténuation (recommandation nº 25).
9. Réévaluer les mesures d'atténuation du risque nº 25 de sorte que la **probabilité résiduelle** de réalisation du risque après l'application des mesures d'atténuation soit réduite (recommandation nº 26).
10. Procéder à une **évaluation des risques relatifs à la sécurité de l'information** et utiliser les solutions techniques existantes prévues dans le système de gestion des dossiers et leurs dispositifs de **sécurité** (recommandation nº 27).

Fait à Bruxelles, le 1er octobre 2020

Wojciech Rafał WIEWIÓROWSKI